DEPARTMENT OF THE ARMY
HEADQUARTERS, 25TH INFANTRY DIVISION
SCHOFIELD BARRACKS, HI 96857-6000

REPLY TO
ATTENTION OF

APVG-CG

5 November 2014

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: 25th Infantry Division Policy Letter 9 - Network Discipline and Security

1. References.

a. DoD Directive 8570.01, Information Assurance Training, Certification, and Workforce Management, 15 August 2004

b. Army Regulation 25-1, Army Information Technology, 25 June 2013

c. Army Regulation 25-2, Information Assurance, 23 March 2009

2. Applicability. This policy applies to all personnel assigned, attached, or under the operational control of 25th Infantry Division, including Department of Defense (DoD) civilian employees, invited contractors, technical representatives, and all family members.

3. Policy. Information Assurance is a commander's program at all levels to implement and enforce. Commanders are charged with ensuring compliance with this policy letter. All personnel are charged with adhering to the specific policy guidance below.

a. All network devices connected to the network or stand alone will comply with the Department of the Army published Information Assurance Vulnerability Management (IAVM) directives and network security policies.

b. All privileged users will be trained and certified IAW DoDD 8570.01 and Army Best Business Practices.

c. All general users will complete the DoD Cyber Awareness Challenge, Portable Electronic Devices and Removable Storage Media, Phishing Awareness, Safe Home Computing, Personally Identifiable Information (PII) courses as well as sign the Acceptable Use Policy (AUP) located at Fort Gordon Information Assurance Training Center website (ia.signal.army.mil).

d. All information assurance incidents whether suspected or in fact will be reported through their respective Information Assurance Security Officer (IASO) to the 25th Infantry Division Information Assurance Manager (IAM).

e. All computers, laptops and media will be Data-At-Rest (DAR) compliant, will be labeled with the appropriate level of classification, and will be government furnished equipment. Virtual Private Network (VPN) accounts require a DAR compliance check of portable electronic devices before use outside of the ordinary office environment.

f. No personally owned computer devices or portable electronic devices (PEDs) are allowed on the network regardless of situation. PEDs include cell phones, smart phones, iPhones, tablets, and mp3 players.

g. All user accounts will be disabled upon Permanent Change of Station (PCS) or Expiration of Term of Service (ETS).

h. Personally Identifiable Information (PII) will be encrypted when contained within an e-mail or removed from a government facility. PII is any information about an individual that is private or intimate to the individual and as distinguished from information related solely to the individual's official functions or public life. This information includes, but is not limited to, any personal information which is linked or linkable to an individual, such as education, financial transactions, medical history, criminal or employment history, and information which can be used to distinguish or trace an individual's identity. Examples include social security numbers, date and place of birth, mother's maiden name, and electronic medical records.

i. No malicious/unauthorized software (i.e. Peer-to-Peer downloads, Instant Messaging, or games) are allowed on government furnished information systems if not explicitly approved by the 25th Infantry Division IAM.

j. No unauthorized installation or removal of programs, disabling of security configurations or audit logs, altering system configurations, straining, testing, circumventing, or bypassing security mechanisms to include enabling the external storage devices unless explicitly permitted by the 25th Infantry Division IAM.

k. Failure to follow any of the above procedures, proper security and regulations will result in immediate suspension of network access and privileges. Commanders at their level may choose to utilize UCMJ authority if the circumstances of the violation fit the criteria.

(1) First Offense – Memorandum signed by the first commander/director in the chain of
command that is in the grade of 05, GS14/GG14/GM14, or NSPS Pay Band 3 or higher. The account may be reactivated once the memo has been received and accepted by 25th Infantry Division IAM.

(2) Second Offense – Memorandum signed by the first commander/director in the chain

of command that is in the grade of 06, GS15/GG15/GM15, or NSPS Pay Band 3 or higher. The account may be reactivated once the memo has been received and accepted by the 25th Infantry Division IAM, along with an automatic 15 day account suspension.

(3) Third Offense – Memorandum signed by the first General Officer or SES in the chain
of command. The account may be reactivated once memo has been received and accepted by 25th Infantry Division IAM, along with an automatic 30 day account suspension.

(4) Any personal electronic devices connected to any Classified network will be confiscated and turned in for processing by the Regional Cyber Center. Any incident involving this nature will undergo a 15-6 investigation. After the conclusion of the investigation, despite the results, the personal electronic device will not be returned to the owner and will be processed by the US Army for proper disposal.

4. Expiration: This 25th Infantry Division Command Policy Memorandum will remain in effect until superseded or rescinded.

5. The point of contact for this memorandum is LTC Joe Pishock, Division G6, at (808) 655-0025.

Tropic Lightning!

CHARLES FLYNN
Major General, USA
Commanding

DISTRIBUTION:
A